A Cyber Security Risk Assessment of Hospital Infrastructure including TLS/SSL and other Threats

A Cyber Security Risk Assessment of Hospital Infrastructure including TLS/SSL and other Threats

Stuart Millar, *PhD Cyber Security Researcher, 13616005, Queen's University of Belfast*
smillar09@qub.ac.uk

***Abstract*— Cyber threats traditionally target governments, financial institutions and businesses. However, of growing concern is the threat to healthcare organizations. This study conducts a cyber security risk assessment of a theoretical hospital environment, to include TLS/SSL, which is an encryption protocol for network communications, plus other physical, logical and human threats. Despite significant budgets in the UK for the NHS, the spend on cyber security appears worryingly low and many hospitals are wide open to attack. This paper concludes that major change, led nationally by the UK government, is needed to make cyber security a major priority in the NHS, without diluting long-standing values of service provision to patients.**

***Index Terms*— health information management, hospitals, information security, network security, public healthcare, risk analysis, security.**

I. Introduction

In 2015 a Sophos survey found the NHS was the biggest victim in the UK of data breaches [13]. Previous attacks on hospitals have caused cancelled operations [12], and more than sixty UK cyber incidents led to personal data breaches in 2015 [1]. In the US, hospitals have been shut down by hackers demanding ransoms [2] and it is said that health-care data is worth up to twenty times the value of credit card details [3]. Furthermore, recent media coverage highlighted the lack of spend in England by the NHS on cybersecurity [1] and the resulting risk to patients and their sensitive personal data. Out-of-date TLS/SSL implementations were discovered. Hence it was decided to research more closely the cyber threats in this specific healthcare environment via a risk assessment. It is felt this underspend is not due to budget constraints, but perhaps because security studies thus far have been insufficient to generate a sound argument for negotiating larger, more impactful sums of money. Public opinion influences government to focus on traditional patient care and service delivery issues rather than the difficult area of cyber security. By the time the public at large falls victim to a serious attack, it will be too late.

In this paper a risk assessment is conducted using ISO 27005:2011 [5], a standard for Information Security Risk Management, and we reference the National Institute of Standards and Technology (NIST) Special Publication 800-37r1 [11], which contains the NIST Risk Management Framework (RMF). The NIST RMF is a US standard for risk assessment for federal systems. With the stakes high in healthcare, these stringent federal standards are considered relevant to this analysis. Our study includes TLS/SSL and we reference the TLS attacks and mitigations detailed in the Internet Engineering Task Force (IETF) RFC7457 [6]. The terms TLS and SSL are interchangeable in this paper. Studying the full list of TLS vulnerabilities is excessive – over three hundred results can found by searching for the TLS keyword on the Common Vulnerabilities and Exposures (CVE) online database [10]. This study is limited to four pages plus appendices, so it not possible to be exhaustive.

II. System Outline – A Theoretical Hospital IT Infrastructure

The focus of this risk assessment is a hospital's IT infrastructure, including traditional system components and also emerging components which, as they become more commonplace, cause the size of the attack surface to increase.

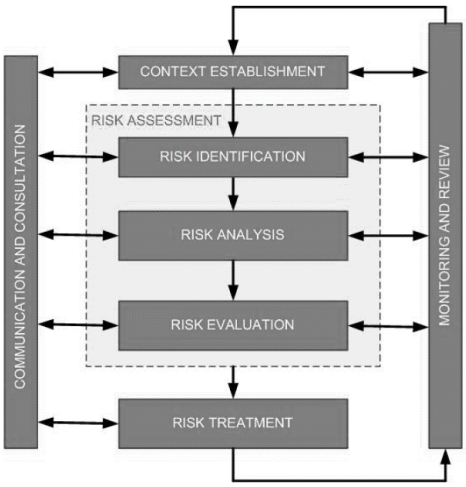
We make a number of assertions, including the use of TLS/SSL. In-house applications are web-based and accessed via single sign-on over a client-server connection, with traffic handled via middleware which uses an implementation of TLS/SSL. Internet of Things (IoT) device to server communications are also encrypted using TLS/SSL. IoT devices can be anything connected the web. Examples of these include surveillance cameras to track patients, medical devices used by doctors, and patient devices like pacemakers or insulin pumps controllable by web interfaces. Portable devices like tablets and mobile phones are used. Patient wellbeing is monitored by wireless and wired systems. A database is hosted in the cloud with patient information and a Voice over Internet Protocol (VoIP) system, where phone communications are passed over the web, is used throughout the hospital with TLS/SSL encrypting those communications. There are system usage constraints concerning personnel, depending on their role and various legal requirements exist that require sensitive personal data to be securely processed and stored. This paper will not detail each piece of legislation a hospital has to adhere to, suffice to say the legal and regulatory obligations are significant.

A detailed information security risk assessment was carried out on this system using ISO 27005:2011[5]. We identify threats to critical system assets and assign values related to

This paper was submitted on 19th December 2016 by Stuart Millar, PhD Cyber Security researcher at the Queen's University of Belfast. Student number 13616005. Email: smillar09@qub.ac.uk

both the consequences of an attack and its likelihood, in order to calculate a risk value, or measure of risk, for each threat. The threats are then ranked by risk value and risk treatment[1] takes place accordingly. Fig. 1 below shows this Risk Management Process, as defined in [5].

Figure 1 – The ISO 27005:2011 risk management process



The NIST Risk Management Framework (RMF) shown in Appendix E and described in [11] is also useful, and this paper refers to it from time to time.

III. Context Establishment

The mission of the NHS in England includes providing "health and high quality care for all" [4]. Implied in this, and also a reasonable public expectation, is that patients are safe and secure when in hospital, as is their medical data.

Firstly, the basic criteria of the assessment need specified. These are the Risk Evaluation criteria, Impact criteria and Risk Acceptance criteria. There is some overlap between these but nevertheless this is an important early step to ensure thoroughness.

1) Risk Evaluation Criteria - risks will be evaluated considering: the strategic value of a given information process, how critical is a given asset, legal obligations, stakeholder expectations, negative impact on reputation and the importance of Confidentiality, Integrity, Availability (CIA), authorization, authentication and non-repudiation.

2) Impact Criteria – impact of a security event will be evaluated considering: financial cost to the organization, effect on business operations, patient risk, reputation damage, legal ramifications and breaches of CIA, authorization, authentication and non-repudiation. There are correlations here between these impact criteria and the NIST RMF, where a system is categorized to determine its impact level. Each data source is analysed for impact of losses of CIA, authorization, authentication, availability and non-repudiation. The highest impact level from these factors is assigned to that data source, and then the highest impact level of all data sources is assigned to the whole system, which feeds into countermeasure selection in the other stages.

3) Risk Acceptance Criteria – consider business criteria, legal and regulatory aspects, operational, technology, financial and social factors. For example, all low-grade risks could be accepted.

Secondly, the scope and boundaries need defined. Our scope includes any IT infrastructure mentioned in the system outline, any elements required for them to operate and any process that requires access to patient data. All assets related to patient data are within scope since stakeholders would expect this end-to-end consideration.

Thirdly, an internal business group for information security risk management needs set up. This defines roles, develops a risk management process, identifies stakeholders and defines escalation though since it is largely an administrative area, it will not be included in this study.

IV. Risk Identification part 1– Assets & consequences

Here we identify what causes a potential loss – how it happens, where it happens and why it happens. The assets within our scope need be identified. An asset is anything that has value to the organization and needs protection. This process results in a list of critical system assets to be risk-managed. These assets underpin primary hospital information, processes and activities. If critical system assets are compromised, then these processes and activities fail or degrade. For example, patient operations are cancelled, monitoring of vital signs interrupted, or administrative functions slowed.

Values are placed on assets relative to the consequences of a security incident. The terms asset value and consequence value are interchangeable. These consequences are disclosure (damage to confidentiality), modification (damage to integrity, authenticity, non-repudiation and accountability), non-availability, and destruction (damage to availability and reliability). Replacement cost is also a factor, as are dependencies, where the more important or numerous the business processes supported by an asset, the greater the asset value. Finally, the impact criteria defined in the previous section are also considered when deciding this valuation. For the asset and consequence valuation we use a scale of 1-5, where 1 = negligible, 2 = low, 3 = medium, 4 = high and 5 = critical.

A high level view of the system components from an attacker's point of view can be seen in Appendix A, and the full list of critical system assets can be found in Appendix B. Already at this stage we are undertaking some risk analysis, since we are assessing the consequences and assigning values accordingly.

The assets are placed in one of four categories – data, hardware, software, and network. It could be argued that patient data, which is anything that can identify an individual patient and all sensitive personal data relating to them and their wellbeing, is of utmost importance, though here are three more examples:

[1] Risk Treatment is the process of selecting and implementing of measures to modify risk

1) TLS/SSL protocol (Network) – as shown in Appendix A, the use of TLS/SSL is considerable, handling web and network traffic, IoT communications, and encryption for VoIP. Considering the consequences of a successful attack on this protocol, we can say disclosure, violation of legislation, loss of trust, personal information breaches, system non-availability, data modification and data destruction are all possible. So, along with the considerable other assets that rely on this protocol, it is valued at 5, or critical.

2) Patient IoT devices (Hardware) – these are, for example, pacemakers and insulin pumps, which are connected to the network for monitoring and automation. If these are attacked, then there is a risk of patient death, data modification, system non-availability and they are expensive to replace. Hence this asset is also valued at 5, or critical.

3) USB sticks (Hardware) – if they were the target of an attack, and contained sensitive personal data, this data is then open to disclosure and modification. There is no direct threat to patient life, and there are few, if any, other assets that rely on a USB stick. They are also not expensive to replace if rendered unusable. So they are given a value of 3, or medium.

V. Risk Identification part 2 – Threats & Vulnerabilities

The next step is identifying threats and their sources to define the overall attack surface. Threats potentially harm assets and can be deliberate or accidental, occurring from internal and external sources. It is useful to consider threat catalogues from 3rd parties, such as Annex C in [5]. The threat scenario list for our hospital system can be found in Appendix C. These scenarios implicitly contain vulnerability details, so vulnerability identification was not treated as a completely separate step. There are three main types of threat - physical, logical and human:

1) Physical threats – target physical system components, like unauthorized tampering and modification of a device. For example, if an attacker gains physical access to an IoT device via a USB port, then malicious firmware could be installed, or some physical functions disabled, or the device itself simply damaged beyond repair.

2) Logical threats – target software or the system. This includes vulnerabilities with TLS. For example, if TLS is used with most non-Diffie-Hellman[2] cipher suites, it is possible to obtain the server's private key to decrypt any session. Or Denial of Service (DoS) attacks can occur where malicious groups of clients called botnets can take a target offline. IoT devices are particularly vulnerable as they are resource constrained with limited memory and battery power. The logical threats of an attack surface can be considerable so if needed they can be categorized as per guidance from the Open Web Application Security Project (OWASP) [14]. These categories are: login/authentication points, admin interfaces, data entry forms, valuable data itself, files from outside the network and lastly security code related to encryption, access control and session management.

3) Human threats – [5] states particular attention should be paid to human threats. Insider threats are the most difficult to defend against. They can be manifested as poorly trained, malicious, negligent, or terminated employees committing computer abuse, theft, using malicious code, selling information and gaining unauthorized system access. Human threats can also originate from hackers trying to get data for illegal disclosure, or terrorists attacking specific medical devices connected to patients with risk of death - there were patents processed in 2013 for insulin pumps which can be controlled from web interfaces [7] and in 2008 doctors disabled the wireless capability in a US politician's pacemaker to thwart assassination attempts [8].

VI. Risk Analysis & Risk Evaluation

To rank the threats in Appendix C for risk treatment, the risk value or measure of risk is needed. This is calculated as follows:

Measure of Risk = Consequence (or Asset) value x Likelihood

When valuing likelihood, thought needs given to how often a threat may occur, the effort and technical skill needed, and the possible impact, all of which form an important part of the risk analysis. We shall use values from 1-5, where 1 = very unlikely, 2 = unlikely, 3 = possible, 4 = likely and 5 = very likely. The estimated occurrence rates are relative to each other. For example, one hospital may only have an attempt to hack its Wi-Fi made once a month, but if it happens to one hundred hospitals, every month, then we can say it is regular. The full list of threat scenarios with likelihoods can be seen in Appendix C. Three examples are:

1) TLS threat scenarios – to exploit these, considerable technical knowledge or computing power is required compared to, say, spreading malware via phishing emails. So the estimated occurrence rate of most of these is 'rarely', the ease of exploit 'hard' and the likelihood is 1, or very unlikely. The exception is threat scenario 15.10 for implementation issues which are much easier to exploit compared to direct flaws in the TLS protocol.

2) Email misuse, either deliberate or accidental by an insider – for example sending documents without security protection, or emailing a large number of recipients deliberately with malicious intent. Since not a lot of technical skill is required and email is used daily by hospital staff, we can say the rate of

[2] The Diffie-Hellman protocol is a method for two computer users to generate a shared private key with which they can then exchange information across an insecure channel.

occurrence is ‘very frequently’, the ease of exploit ‘easy’ and therefore logically the likelihood is 5, very likely.

3) Attempting to kill or harm patients through terrorist or political motivations by attacking implanted IoT devices – a successful attack like this has not been reported, though there may well have been failed attempts. It is an attractive option to a terrorist attacker. The technical nous required is considerable, therefore the rate of occurrence is ‘rarely’, the ease of exploit ‘hard’, and we say the likelihood is 2, unlikely.

Using the aforementioned equation for measuring risk, we can quickly determine risk values and rank the threats to continue the risk analysis. The table showing the final ranked threats in order of priority can be found in Appendix D.

VII. Risk Treatment

Four options exist for risk treatment – risk modification using controls, risk retention, risk avoidance and risk sharing.

Controls are selected in order to reduce risks to an acceptable level, known as residual risk. These controls are listed in Appendix D. Risk retention accepts risks as per the acceptance criteria specified in the context establishment.

Our focus in this paper is solely the high-priority risks with a risk value of 20 or higher. There are however interesting evaluations that can be made for lower priority risks. For example, the threat of death to patients through IoT implanted device tampering sounds severe but when evaluated the likelihood is so low that the risk is accepted as the technical skill needed is significant. From reviewing the threat scenarios in Appendix C, risk avoidance, where activities that create risks should be removed, and risk sharing, where the risk is outsourced to a 3rd party for handling, are not required.

The controls selected should be based on a cost/benefit ratio unless a risk is particularly severe, in which case economic grounds are less important. If the NIST approach is followed to the letter, there is a list of minimum controls for high impact systems like ours. Controls were picked from the families listed in [11], a summary of which forms Appendix F. Detailing every required NIST control would be excessive.

The full list of selected controls for high-priority risks can be found in Appendix D, including those relating to the implementation of TLS/SSL. The TLS vulnerabilities were compiled from [6], which details specific mitigations. In our risk assessment, the highest ranked TLS threat arose from implementation, which historically has been the case, for example with the Heartbleed[3] bug in OpenSSL. We will not repeat all the non-implementation based mitigations here, though some key ones are disabling TLS compression to prevent TIME[4] attacks, and ensuring use of cipher suites that offer forward secrecy, where revealing a private key does not expose past or future sessions to a passive attacker. Three examples of controls from Appendix D are given below:

1) Theft of information from database by an insider – removing temporary or emergency accounts (which may have weaker passwords) reduces entry points for an insider without credentials, as does automatic lock out after the threshold for unsuccessful logon attempts has been reached, either from manual or brute-force attempts. Security training reduces the likelihood of information theft by abuse of unattended PCs, and citizenship requirements for access, whilst controversial, may be effective. Tools can be used for monitoring network traffic for signs of information theft, and certain sites with a history of posting of stolen data can be monitored, although that doesn’t directly prevent the initial insider theft.

2) Wi-Fi hacking – this supports many other assets, as per Appendix A. Intrusion Detection Systems (IDS) create alerts when a compromise has taken place. Wireless link protection prevents the network being taken down by electromagnetic signal interference. Physical access controls prevent tampering with hardware, whilst encryption is important with older protocols like WEP being vastly inferior and easy to crack compared to standards like AES.

3) Malware installation – security awareness training with practical exercises about handling suspicious emails (a major source of malware) and the threat of social engineering strengthens front-line defences. Least privilege and least functionality prevent program execution. Alerts can be setup for unauthorized software installation, and monitoring communications traffic means that unusual behavior, like spikes in outbound traffic caused by malware, can be detected.

Controls need reviewed regularly. Over time, the capability of attackers increases, like the example concerning medical IoT implanted devices. The monitoring of risks has to take place iteratively to account for changes in assets, the organization, the law, or the emergence of new vulnerabilities and threats. As per Fig. 1, communication and consultation also take place iteratively.

Estimated costs have been assigned to the countermeasures for the high-priority risks. Higher costs tend to be associated with extra physical protection, however low cost countermeasures are no less important. They involve combining a lot of granular controls to benefit from synergy. For example, combing security training, removing default accounts, monitoring network traffic and unsuccessful logins, citizenship requirements and dealing with terminated employee access can be combined to mitigate insider threats. Individually, these are not expensive controls, relative to, say, 24-hour surveillance of servers and network infrastructure.

VIII. Conclusions & Future Work

The threat to human life is the ultimate threat. The government budget for NHS England for 2016-20 is upwards

[3] Heartbleed is a vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing information protected, under normal conditions, by the TLS/SSL encryption used to secure the Internet.

[4] A TIME (Timing Info-leak Made Easy) attack is where a payload is inferred from transmission time.

of £100billion annually. The average spend for an NHS England trust in 2015 was £20,000[1]. Hence there is a major underspend and the cost of countermeasures should not ultimately prevent implementation. Therefore, the threshold for ruling out countermeasures or delaying implementation for financial reasons should be higher than that of other sectors. Our threat mitigation strategy is that all the controls identified in Appendix C should be implemented. Threats arising from use of poor implementations of TLS/SSL are significant but can be mitigated by a collection of low-cost steps as we have outlined, again in Appendix C.

For future work we would like to investigate occurrences of out-of-date TLS/SSL use and server certificates across the NHS to build a detailed proof-of-concept vulnerability picture. In the 2016-17 mandate to NHS England from the Department of Health, there is only one objective related to cyber security which reads "Robust data security standards in place and being enforced for patient confidential data" [9]. This level of detail is inadequate and serious change is required to bring cyber security to the very top of the agenda in the NHS, without sacrificing the delivery of patient care.

Acknowledgement

This paper was supported by the Centre for Secure Information Technologies (CSIT), at the Queen's University of Belfast.

References

[1] T. Cheshire, "NHS patients being put 'at risk' because of cybersecurity flaws", Sky News, Wed 16th November 2016, http://news.sky.com/story/nhs-patients-being-put-at-risk-because-of-cybersecurity-flaws-10657537

[2] A. Balakrishnan, "The hospital held hostage by hackers", CNBC, Wed 16th February 2016, http://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html

[3] C. Young, "Why hackers want your health-care data", CNBC, Wed 27th May 2015, http://www.cnbc.com/2015/05/27/why-hackers-want-your-health-care-data-commentary.html

[4] NHS England, "Our Vision and Purpose", https://www.england.nhs.uk/about/our-vision-and-purpose/

[5] BS ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management, 2011, ISBN 9780580717147

[6] Y. Sheffer, R. Holz, P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", Internet Engineering Task Force (IETF) RFC 7457, ISSN 2070-1721, https://tools.ietf.org/html/rfc7457

[7] E. Basu, "Hacking Insulin Pumps and Other Medical Devices From Black Hat", Forbes, http://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical- devices-reality-not-fiction/#35478e934327

[8] L. Vaas, "Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking", Sophos, 22nd October 2013, https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/

[9] Department of Health, "The Government's mandate to NHS England for 2016-17", January 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/494485/NHSE_mandate_16-17_22_Jan.pdf

[10] Common Vulnerabilities and Exposures, TLS, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=TLS

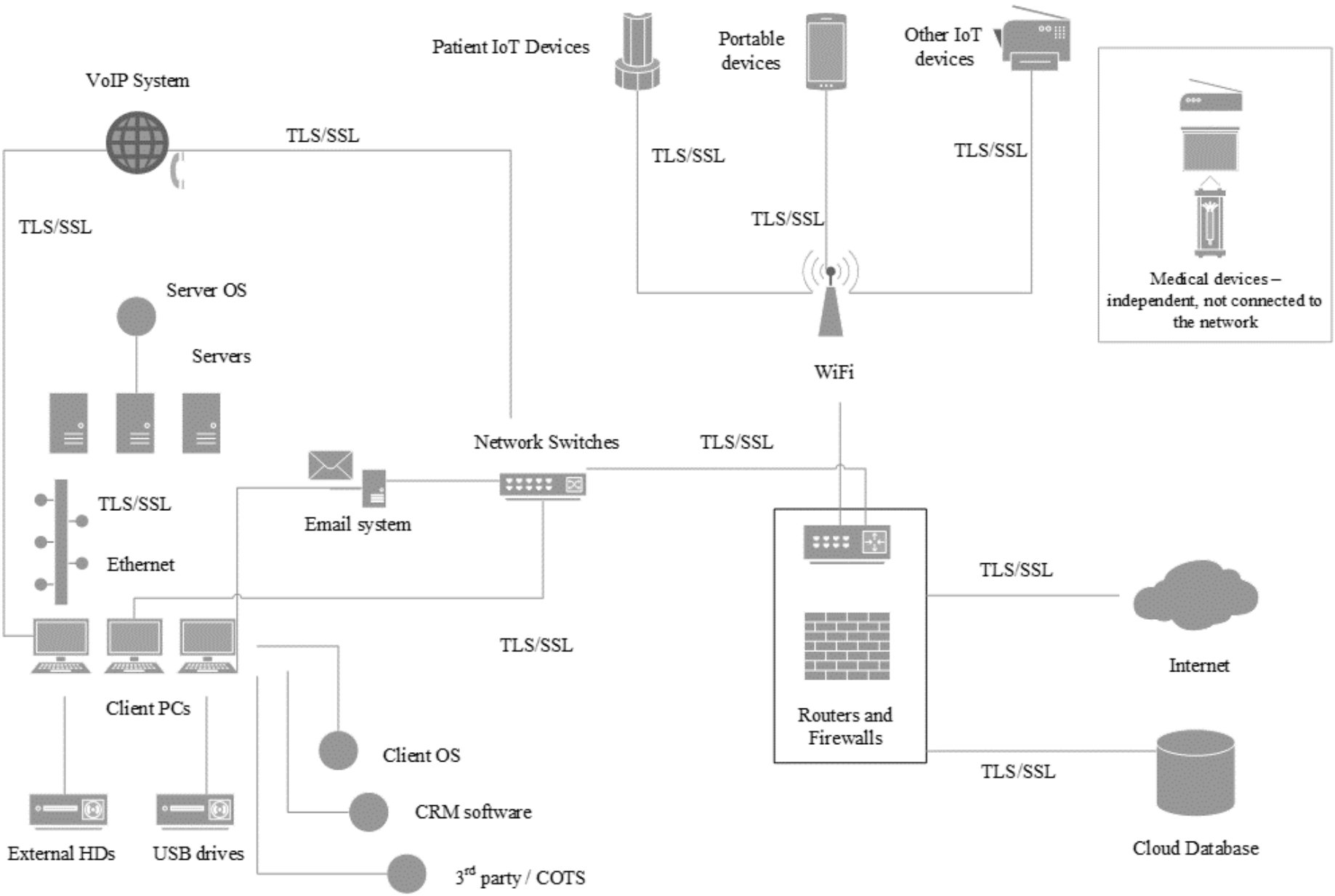
[11] National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations", April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[12] BBC News, "Lincolnshire operations cancelled after network attack", 31st October 2016, http://www.bbc.co.uk/news/uk-england-humber-37822084

[13] L. Evenstad, "NHS IT managers think security better than it is, survey finds", ComputerWeekly.com, 21st January 2016, http://www.computerweekly.com/news/4500271466/NHS-IT-managersthinksecurity-better-than-it-is-survey-finds

[14] Open Web Application Security Project, OWASP, "Measuring and Assessing the Attack Surface", https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet#Measuring_and_Assessing_the_Attack_Surface

Appendix A – High level view of hospital system components from an attacker's perspective



Note the extensive use of TLS/SSL for encrypting communications

Appendix B – Critical System Assets including valuation (1 = negligible, 2 = low, 3 = medium, 4 = high and 5 = critical)

Category	Asset	Comments / Considerations / Key Consequences	Asset AKA Consequence Valuation	Last Reviewed
Data	Patient Data	Anything that can identify an individual patient and all sensitive personal data relating to that patient, either for identifying them, or in relation to any aspect of their health and wellbeing. Disclosure, modification and destruction.	5	13/12/2016
Hardware	Client PCs	Impaired business performance through non-availability, disclosure and modification.	4	13/12/2016
Hardware	Server Farm	Impaired business performance through non-availability, disclosure, modification and cost of replacement.	5	13/12/2016
Hardware	Portable devices	Laptops, mobile phones, tablets, etc. Disclosure, modification and non-availability.	3	13/12/2016
Hardware	Medical devices	Independent devices for patient data collection, not connected to the network. Disclosure, modification and cost of replacement.	4	13/12/2016
Hardware	External hard disks	Disclosure, modification, non-availability.	3	13/12/2016
Hardware	USBs	Disclosure and modification.	3	13/12/2016
Hardware	Patient IoT Devices	For example, pacemakers, insulin pumps, possibly drips. These are treatment devices connected to the network. Personal safety, risk of death, modification, non-availability and cost of replacement.	5	13/12/2016
Hardware	Other IoT Devices	For example, surveillance cameras, IoT devices specifically for patient data collection which are connected to the network	4	13/12/2016
Software	Cloud Database	Non-availability, disclosure, violation of legislation, loss of trust, personal information breach, data modification and destruction are key consequences.	5	13/12/2016
Software	CRM software	Non-availability, impaired business performance, disclosure and data modification are key consequences.	3	13/12/2016
Software	Middleware	This impacts a lot of other system assets. Disclosure, modification and non-availability are key consequences.	5	13/12/2016
Software	VoIP software	Disclosure of data, conversations and non-availability are key consequences.	3	13/12/2016
Software	Email system	Disclosure, modification, non-availability	4	13/12/2016

Software	Operating Systems on client PCs and servers	Non-availability, disclosure and modification.	3	13/12/2016
Software	All other 3rd party / COTS software	Non-availability, disclosure and modification.	3	13/12/2016
Software	TLS/SSL implementation	For example, OpenSSL for electronic messaging using cryptography. Implementations are classified as software as per ISO 27000:2011. Non-availability, disclosure, violation of legislation, loss of trust, personal information breach, data modification, destruction of data.	5	13/12/2016
Network	Network infrastructure	Like switches and routers. Non-availability, disclosure, violation of legislation, loss of trust, personal information breach, data modification and destruction are key consequences.	5	13/12/2016
Network	Ethernet Connections	Carries data encrypted by TLS/SSL over a physical wire. Non-availability, disclosure, violation of legislation, loss of trust, personal information breach, data modification and destruction are key consequences.	5	13/12/2016
Network	TLS/SSL protocol	Non-availability, disclosure, violation of legislation, loss of trust, personal information breach, data modification and destruction are key consequences.	5	13/12/2016
Network	Wi-Fi	Carries data encrypted by TLS/SSL using wireless protocols. Non-availability, disclosure, violation of legislation, loss of trust, personal information breach, data modification and destruction are key consequences.	5	13/12/2016

Appendix C – Threat scenarios, including estimated occurrence rate, ease of exploit and likelihood value (1 = very unlikely, 2 = unlikely, 3 = possible, 4 = likely and 5 = very likely)

Threat type	**Threat ID**	**Scenario Details**	**Estimated Occurrence Rate**	**Ease of Exploit**	**Likelihood**
Physical	1	IoT device tampering via USB port, applies to relevant patient IoT devices and others IoT devices.	Rarely	Medium	3
Physical	2	Unauthorised access to server room and network hardware.	Occasionally	Easy	5
Physical	3	Tampering with medical devices not connected to network.	Occasionally	Easy	4
Physical	4	Side-channel timing attack on the middleware and hardware that is performing encryption for TLS/SSL in order to deduce keys.	Occasionally	Hard	2
Physical	5	Wi-Fi signal jamming.	Occasionally	Medium	3
Physical	6	Network tap or full duplex devices installed between host and switch.	Rarely	Hard	1
Logical	7	Packet capturing tools used to intercept and log network traffic. Traffic captured at host, or port mirroring (copying all traffic to or from a user port to an attacker's port).	Occasionally	Hard	5
Logical	8	Active attacks: replay attack, message modification Man-In-The-Middle (MITM), Denial of Service (DoS), masquerade (spoofing source IP address)	Occasionally	Medium	3
Logical	9	Passive attacks: eavesdrop to get message contents, traffic analysis (subtle, even with encryption), studying metadata.	Occasionally	Easy	5
Logical	10	Network threats and attacks – actual session hijacking e.g. MITM	Rarely	Medium	3
Logical	11	Access to web interfaces that are left public, when they should be private, to misuse system components. Like a User Interface detailing patient information or to control a medical device.	Occasionally	Easy	3
Logical	12	Wi-Fi hacking – where the wireless network is hacked in order to sniff traffic or carry out other malicious activity.	Very frequently	Easy	5
Logical	13	Brute force attacks using computer power to try password variations on web-facing logins to gain access.	Regularly	Easy	5

Logical	14	Malware installation, e.g. by phishing emails / social engineering	Very frequently	Easy	5
Logical	15.1	TLS - SSL stripping – where HTTP traffic and HTML pages are modified on the wire. Only effective on the web if the client initially accesses a webserver using HTTP. All the traffic from the victim's machine is routed via a proxy the attacker creates. This is a MITM attack where the communications become plain text which is sniffable, and information can be collected. Instead of accessing https://site.com, a user accesses http://site.com. So if using our intranet, which is protected by TLS, then the attacker could for example sniff traffic and gain sensitive personal data.	Rarely	Hard	2
Logical	15.2	TLS - STARTTLS command injection attack (CVE-2011-0411) – this command upgrades a cleartext connection to use TLS. However, the application layer input buffer can retain commands that were pipelined with the STARTTLS command. If they are malicious commands, then the results could be serious.	Rarely	Hard	2
Logical	15.3	TLS - BEAST (Browser Exploit Against SSL/TLS) attack (CVE-2011-3389) – there are problems with the TLS 1.0 implementation of Cipher Block Chaining (CBC) to decrypt parts of a packet and decrypt HTTP cookies when HTTP is run over TLS. It allows attackers to silently decrypt data that is passing between a webserver and an end-user browser.	Rarely	Hard	2
Logical	15.4	TLS - Attacks on RC4 – RC4 is a cipher used with TLS for many years. It has cryptographic weaknesses though. Recent cryptanalysis studies exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts. These results are close to being practically exploitable – as of Feb 2015 they require 2^26 sessions or 13x2^30 encryptions. So they are feasible but not practical due to the amount of traffic needed to mount the attacks. RC4 is no longer seen as providing a sufficient level of security for TLS sessions.	Rarely	Hard	2
Logical	15.5	TLS - Compression Attacks: CRIME (CVE-2012-4929), TIME and BREACH – CRIME allows an attacker to decrypt ciphertext (specifically cookies), when TLS is used with TLS-level compression. TIME and BREACH attacks are similar when TLS is used with http-level compression.	Rarely	Hard	2
Logical	15.6	TLS - Certificate and RSA-related attacks – using RSA certs means exploitable timing issues	Rarely	Hard	2
Logical	15.7	TLS - Theft of RSA private keys – if TLS is used with most non-Diffie-Hellman cipher suites, it is possible to obtain the server's private key to decrypt any session. Wireshark does this to inspect TLS-protected connections.	Rarely	Hard	2

Logical	15.8	TLS - Renegotiation (CVE-2009-3555) – a major attack on the TLS renegotiation mechanism applies to all current versions of the protocol. Here the attacker forms a TLS connection with the target server, injects content of their choice, then splices in new TLS connection from a client, which is treated as a renegotiation, and the server believes the initial data transmitted by the attacker is from the same entity as the subsequent client data.	Rarely	Hard	2
Logical	15.9	TLS - Denial of Service – malicious clients and groups of clients called botnets can mount denial-of-service attacks. Particularly with regard IoT devices, since they are resource constrained devices, which makes them easier to attack and also easier to create a botnet from.	Occasionally	Easy	2
Logical	15.10	TLS - Implementation issues – even when TLS is properly specified, the implementation can be incorrect, for example there are well known issues with OpenSSL, such as Heartbleed. The implementations can omit validating server certificates for example.	Occasionally	Easy	4
Human	16	Theft of information from database by an insider.	Occasionally	Easy	5
Human	17	Theft of mobile devices or other digital media by an insider.	Occasionally	Easy	5
Human	18	Email misuse, either deliberate or accidental by an insider.	Very frequently	Easy	5
Human	19	Deliberate or accidental tampering with of non-network connected devices.	Occasionally	Easy	5
Human		Accidental or deliberate spreading of malware from USB drives, external HDs etc that infect a client which then infects the network.	Occasionally	Easy	5
Human	20	Unauthorised access to servers.	Rarely	Easy	5
Human	21	Accidental or deliberate information disclosure.	Very frequently	Easy	5
Human	22	Attempt to kill or harm patients through terrorist or political motivations by affecting implanted IoT devices.	Rarely	Hard	1
Human	23	Unauthorised system access from a hacker to gain information for financial gain, illegal information disclosure or destroying records.	Rarely	Medium	3
Human	24	Industrial espionage for some economic benefit.	Rarely	Medium	1

Appendix D – Threat scenario ranking including risk value, controls and cost

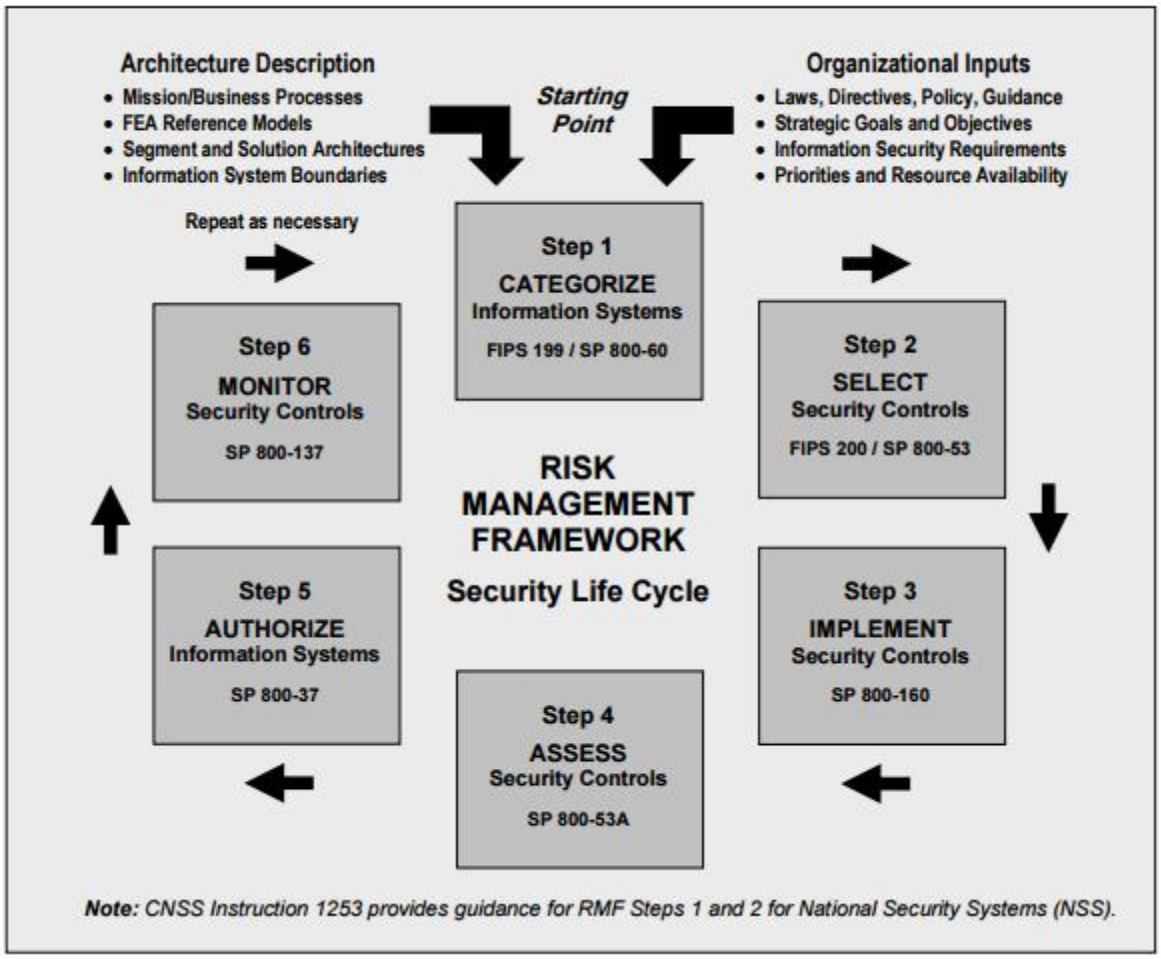
Threat ID	Consequence /Asset Value	Likelihood	Risk Value	Threat Ranking	Scenario Details	Controls	Cost
2	5	5	25	1	Unauthorised access to server room and network hardware	Physical Access Authorizations: Access by position/role, restrict unescorted access. Physical Access Control: Continuous alarms/monitoring, lockable casings, tamper protection. Monitoring Physical Access: intrusion alarms/surveillance equipment, video surveillance, monitoring physical access to information systems.	High
7	5	5	25	1	Packet capturing tools used to intercept and log network traffic. Traffic captured at host, or port mirroring (copying all traffic to or from a user port to an attacker's port).	Boundary protection: Protects against unauthorized physical connections. Transmission Confidentiality and Integrity: cryptographic and physical protection. Information System Monitoring: Automated response to suspicious events	Medium
9	5	5	25	1	Passive attacks: eavesdrop to get message contents, traffic analysis (subtle, even with encryption), studying metadata.	Boundary protection: Protects against unauthorized physical connections. Transmission Confidentiality and Integrity: cryptographic and physical protection. Information System Monitoring: Automated response to suspicious events	Medium
12	5	5	25	1	Wi-Fi hacking – where the wireless network is hacked in order to sniff traffic or carry out other malicious activity.	Information System Monitoring: Wireless Intrusion Detection, system-wide intrusion detection system. Wireless Link Protection: against electromagnetic interference, reduce detection potential. Physical Access Control: Lockable cases, tamper protection. Wireless Access: Authentication and encryption (ensure WEP is not used, prefer AES.), monitor unauthorised connections, restrict configuration by users, antennas / transmission power levels	High

16	5	5	25	1	Theft of information from database by an insider.	Account Management: Removal of temporary / emergency accounts, inactivity logout, account monitoring, disable accounts for high-risk individuals. Unsuccessful Logon Attempts: Automatic account lock. Previous Logon Notification: Successful / unsuccessful logons. Remote Access: monitoring for unauthorized connections. Security Awareness Training: Insider threat. Information System Monitoring: System-wide intrusion detection system. Analyse communications traffic anomalies. Maintenance Personnel: control access from individuals without appropriate access. Citizenship requirements for classified systems. Identification and authentication policy and procedures: ensure vigilance for organisational users and those external to the organisation also. Monitoring for information disclosure: use of automated tools, review of monitored sites.	Low
20	5	5	25	1	Unauthorised access to servers.	Physical Access Authorizations: Access by position/role, restrict unescorted access. Physical Access Control: Continuous alarms/monitoring, lockable casings, tamper protection. Monitoring Physical Access: intrusion alarms/surveillance equipment, video surveillance, monitoring physical access to information systems.	High
21	5	5	25	1	Accidental or deliberate information disclosure.	Access Enforcement: role-based access control. Revocation of access authorizations. Security Awareness Training: Insider threat. Monitoring for information disclosure: Use of automated tools, review of monitored sites. Protection of information at Rest: cryptographic protection. Transmission Confidentiality and Integrity: Cryptographic protection. Personnel Termination & Access Agreements: post-employment requirements.	Medium

14	4	5	20	2	Malware installation, e.g. by phishing emails / social engineering	Least Privilege: Prohibit non-privileged users from executed privileged functions. Security Awareness Training: Practical exercises for phishing, social engineering. Least functionality: prevent program execution, unauthorised software/blacklisting. Software usage restrictions: open source software. User-installed software: alerts for unauthorised installations, prohibit installation without privileged status. Malicious Code Protection: updates only by privileged users, detect unauthorised commands. Information System Monitoring: inbound and outbound communications traffic. Spam Protection: central management, continuous learning capability.	Low
15.10	5	4	20	2	TLS - Implementation issues – even when TLS is properly specified, the implementation can be incorrect, for example there are well known issues with OpenSSL, such as Heartbleed. The implementations can omit validating server certificates for example.	Implement the mitigations in the RFC. Ensure implementations are kept-up to date so latest vulnerability fixes are in place. Malicious Code Protection: Updates only by privileged users. Flaw Remediation: Removal of previous versions of software/firmware.	Low
18	4	5	20	2	Email misuse, either deliberate or accidental by an insider	Access Enforcement: role-based access control. Revocation of access authorizations. Security Awareness Training: Insider threat. Monitoring for information disclosure: Use of automated tools, review of monitored sites. Transmission Confidentiality and Integrity: Cryptographic protection.	Medium

19	4	5	20	2	Deliberate or accidental tampering with of non-network connected devices.	Maintenance Personnel: restrict individual movement on premises without appropriate access. Physical Access Control: lockable casings, tamper protection. Supply Chain Protection: acquisition methods. Software, firmware and information integrity: tamper evident packaging,	Medium
3	4	4	16	3	Omitted	Omitted – risk value less than 20	
1	5	3	15	4	Omitted	Omitted – risk value less than 20	
5	5	3	15	4	Omitted	Omitted – risk value less than 20	
8	5	3	15	4	Omitted	Omitted – risk value less than 20	
10	5	3	15	4	Omitted	Omitted – risk value less than 20	
13	3	5	15	4	Omitted	Omitted – risk value less than 20	
17	3	5	15	4	Omitted	Omitted – risk value less than 20	
23	5	3	15	4	Omitted	Omitted – risk value less than 20	
4	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.1	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.2	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.3	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.4	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.5	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.6	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.7	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.8	5	2	10	5	Omitted	Omitted – risk value less than 20	
15.9	5	2	10	5	Omitted	Omitted – risk value less than 20	
11	3	3	9	6	Omitted	Omitted – risk value less than 20	
6	5	1	5	7	Omitted	Omitted – risk value less than 20	
22	5	1	5	7	Omitted	Omitted – risk value less than 20	
24	5	1	5	7	Omitted	Omitted – risk value less than 20	

Appendix E – The NIST Risk Management Framework (RMF)



Appendix F – The NIST families of controls

NIST Families of Controls	
Access Control	Media Protection
Awareness Training	Physical and Environmental Protection
Audit and Accountability	Planning
Security Assessment and Authorization	Personnel Security
Configuration Management	Risk Assessment
Contingency Planning	System and Services Acquisition
Identification and Authentication	System and Communications Protection
Incident Response	System and Information Integrity
Maintenance	Program Management